40 Gb/s, secure optical communication based upon fast reconfigurable time domain spectral phase en/decoding with 40 Gchip/s optical code and symbol overlapping

Zhensen Gao,[1] Bo Dai,[1] Xu Wang,[1,*] Nobuyuki Kataoka,[2] and Naoya Wada[2]

[1]*Joint Research Institute for Integrated Systems, Department of Electrical, Electronic & Computer Engineering, Heriot-Watt University, Riccarton, Edinburgh, EH14 4AS, UK*

[2]*Photonic Network Group, National Institute of Information and Communications Technology, Tokyo 184-8795, Japan*

**Corresponding author: x.wang@hw.ac.uk*

Received June 30, 2011; revised September 3, 2011; accepted September 23, 2011; posted October 11, 2011 (Doc. ID 150290); published November 9, 2011

We propose and experimentally demonstrate a 40 Gb/s secure optical communication system with on–off-keying (OOK) modulation format by using a time domain spectral phase en/decoding scheme, which employs a highly dispersive element and high-speed phase modulator for introducing significant symbol overlapping for both the encoded and incorrectly decoded noiselike signals to enhance the information security against eavesdropping using a power detector. The influence of dispersion and chip modulation rate on the symbol overlapping of the incorrectly decoded signal has been analytically investigated and experimentally verified. Security enhancement for 40 Gb/s OOK data using fast reconfigurable 40 Gchip/s optical codes with code lengths of up to 1024 has been demonstrated and compared with a 10 Gb/s system. © 2011 Optical Society of America

OCIS codes: 060.2330, 060.4785, 060.5060.

With the explosive growth of optical network resources, secure optical communication is becoming increasingly important and has recently attracted great research interest [1]. To meet the military or commercial requirement of private data exchange, it is crucial to protect certain confidential data from malicious eavesdropping by an unauthorized party, and therefore special attention should be paid on the security in the deployment of next-generation optical network. Various approaches for secure optical communication have been proposed over the past years, such as quantum key distribution [2], chaotic communication [3], and optical steganography [4]. In addition to those, the optical-code-division-multiple-access (OCDMA) technique based on optical code (OC) processing also has the potential for providing information security [5–7] because the encoded signal by the OC manifests itself like a noise, making the eavesdropper hard to intercept the data.

However, there are several issues in OCDMA systems with on–off-keying (OOK) modulation format. It has been demonstrated that, in an OOK OCDMA system, an eavesdropper can tap the individual user's signal and recover the data by using a simple power detector without the need of knowing the exact OC [5,8]. The eavesdropper may even extract the OC by analyzing the fine structure of the encoded spectrum [8] or waveform [9], and therefore the OOK data security cannot be guaranteed. Also, as one of the key components in an OCDMA system, it is usually desired for the optical en/decoder to generate ultralong OC with rapid reconfigurable capability for the sake of system flexibility and security, but most of the conventional optical en/decoders do not offer these capabilities. Moreover, in many previously demonstrated OCDMA systems, the data rate was mainly restricted within 10 Gb/s [7,10]. It is desirable to operate the OCDMA technique at a data rate beyond 10 Gb/s in a future optical network.

In this Letter, we propose an approach for enhancing the security of high-speed OOK data based on a time domain spectral phase en/decoding (SPE/D) scheme deploying highly dispersive elements and a high-speed phase modulator to introduce significant symbol overlapping for both the encoded and incorrectly decoded noiselike signals whose temporal durations are greater than twice the bit period. A data rate as high as 40 Gb/s has been experimentally demonstrated with 40 Gchip/s, code-length variable OCs of up to 1024 chips. Figure 1 illustrates the experimental setup of the proposed time domain SPE/D scheme with symbol overlapping. The laser source is an actively mode-locked laser diode (MLLD) producing nearly transform-limited 2.8 ps pulses at a repetition rate of 10 GHz and spectrally centered at 1549.8 nm. To investigate the security for different bit rates, both 10 and 40 Gb/s OOK data are used in the

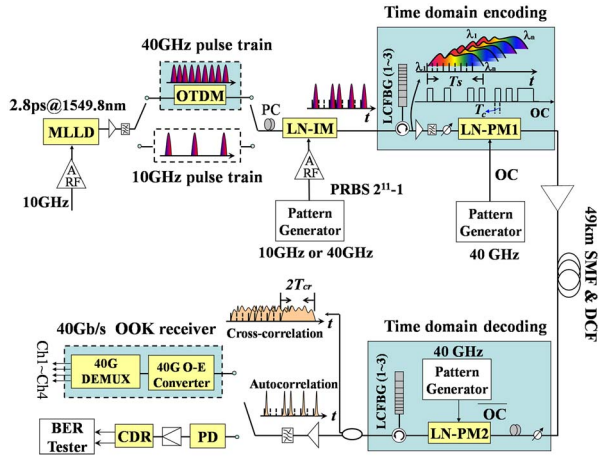

Fig. 1. (Color online) Experimental setup of the 40 Gb/s secure optical communication system. PC, polarization controller.

experiment. The 40 GHz pulse train is generated by multiplexing the 10 GHz pulses using a four-stage planar-lightwave-circuit-based optical time division multiplexer (OTDM). To generate the 10 and 40 Gb/s OOK data, the original pulse train is intensity modulated by a lithium-niobate (LN) intensity modulator driven by a 10 or 40 Gb/s pseudo-random bit sequence (PRBS) of length $2^{11}-1$; a $2^{11}-1$ PRBS generated from a pulse pattern generator and amplified by a radio frequency amplifier (ARF) is used to drive a LN intensity modulator (LN-IM). Then after that, three identical cascaded linearly chirped fiber Bragg gratings (LCFBGs) (each has a 10 dB bandwidth of ~4.7 nm and dispersion slope of ~80 ps/nm) are used to significantly broaden the pulse train. Each bit of the original pulse with a bit period of T_b is broadened within the time duration T_s of ~1128 ps, and hence the adjacent consecutive stretched pulses are significantly overlapped with each other. After the temporal stretching, a 40 GHz LN phase modulator (PM) driven by a 40 Gchip/s, fast reconfigurable and code-length variable pseudo-random OC with chip duration of T_c is used to perform phase modulation on the stretched pulses, which can be regarded as time domain spectral phase encoding. Each stretched pulse will experience a different section of the OC and has a 45-chip spectral phase pattern according to T_s/T_c. A span of 49 km single-mode fiber (SMF) and dispersion compensation fiber (DCF) is used for transmission.

At the receiver side, similar configuration as the encoding part is utilized, but the phase modulator is driven by the complementary code patterns for spectral phase decoding. The synchronization between the optical encoding and decoding sides is essential for decoding the stretched pulse train. A global clock is used throughout the system, and a tunable optical delay line is also employed before the phase modulator to temporally align the complementary spectral phase pattern and the applied OC in the encoding side. After that, another series of LCFBGs with opposite dispersion is used to compress the stretched and spectral phase decoded signal to recover the original pulse. The correctly decoded signal is finally launched into a 10 or 40 Gb/s packet receiver for opto-electro (O-E) conversion. The 10 Gb/s signal can be directly detected by a photodetector (PD) followed by a clock and data recovery circuit (CDR), while, for the detection of 40 Gb/s OOK data, a 40 GHz electrical demultiplexer (DEMUX) is used to demultiplex the 40 Gb/s data into four-channel 10 Gb/s OOK data for measuring the bit error rate (BER).

Figures 2(a) and 2(b) show the spectra of the uncoded and encoded 40 Gb/s OOK signals by a 1024-chip OC, from which it can be seen the encoded spectrum has a distinct profile with the uncoded signal, and it is hard to extract the OC by analyzing the spectral dip. The temporal profile of the stretched 40 Gb/s OOK optical pulses by the LCFBGs is shown in Fig. 2(c). Because of the significant overlapping of ~45 pulses (T_s/T_b) after the stretching, the temporal profile of the overall signal is completely different from its spectrum, and it exhibits as a noise. Unlike traditional OOK systems [5,8], the eavesdropper cannot directly regenerate the original OOK data by simply detecting the power from this noise-like signal for both the 10 and 40 Gb/s data rates. One may assume that the eavesdropper has plenty of resources and knows everything including the chromatic dispersion except the OC, so he can easily compress the stretched pulses and try to intercept the data. However, even if the eavesdropper fabricates identical LCFBGs for temporal compressing, since he does not know the applied OC, he can only get an incorrectly decoded cross-correlation signal with symbol overlapping, which can further enhance the data security. If the time duration of the incorrectly decoded signal for each bit is larger than twice the bit period after temporal compressing, the cross-correlation signal may still spread across the time scale with significant symbol overlapping, and the bit "0" is filled with the encoded signals from the other bits of "1," so it is difficult for the eavesdropper to discriminate the bit symbol by using a simple power detector. The time duration of the incorrectly decoded signal in this scheme is mainly determined by the spectral resolution of each chip, which depends on the chromatic dispersion D (ps/nm) and chip modulation rate R_C (Gchip/s). Assuming that the input pulse is a transform-limited Gaussian pulse with a time-bandwidth product of 0.441 [11], as each chip occupies $1000/(R_C \cdot D)$ nm spectral range, the corresponding FWHM of the cross-correlation signal T_{cr} (ps) can be approximately given by

$$T_{\mathrm{cr}} = \frac{0.8 \cdot 0.441 \cdot R_C \cdot D}{100}.$$

Figure 3(a) depicts the dependence of the T_{cr} with the D and R_C. The two planes are shown as the reference levels of the minimum required T_{cr} to achieve security for 10 and 40 Gb/s. By increasing the total dispersion D and chip modulation rate R_C, the T_{cr} can be greater than the reference level, showing the feasibility of security improvement. Figure 3(b) shows the relationship of the minimum D and R_C when the T_{cr} is on the reference planes, from which one can see that the minimum required D for 10 Gb/s is higher than that of the 40 Gb/s, and the higher the R_C, the lower the minimum

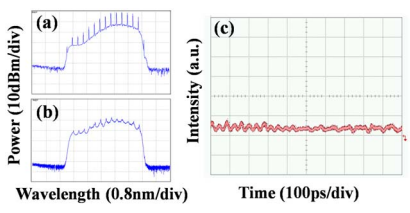

Fig. 2. (Color online) (a), (b) Spectra of the uncoded and encoded signal; (c) temporal profile of the stretched 40 Gb/s OOK pulse train after the LCFBGs.

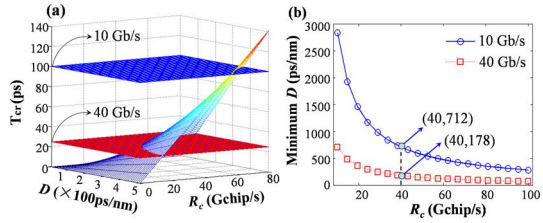

Fig. 3. (Color online) (a) Time duration T_{cr} versus D and R_C; (b) minimum required D versus R_C for 10 and 40 Gb/s.

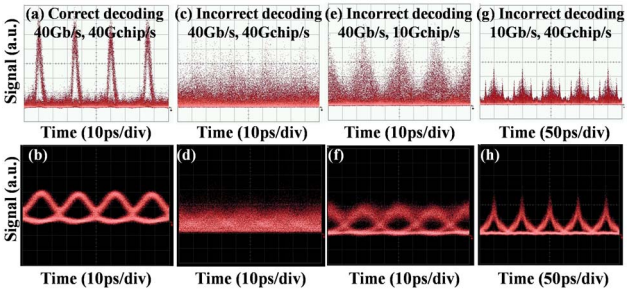

Fig. 4. (Color online) Waveforms and eye diagrams of (a), (b) correct and (c), (d) incorrect decoding for 40 Gb/s, 40 Gchip/s; (e), (f) incorrect decoding for 40 Gb/s, 10 Gchip/s; (g), (h) incorrectly decoded signals for 10 Gb/s, 40 Gchip/s.

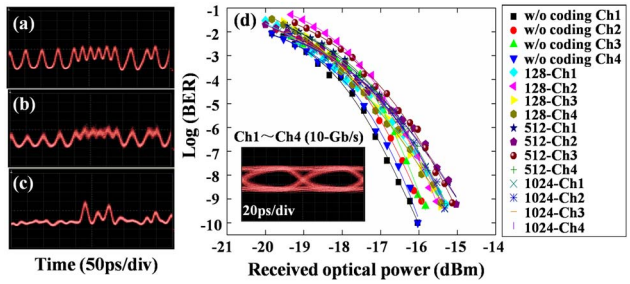

Fig. 5. (Color online) (a) Original pattern; (b), (c) encoded patterns with R_C of 10 and 40 Gchip/s; (d) BER for the four 10 Gb/s tributaries with various OCs.

D. Because of the modulation speed limitation of a commercially available phase modulator, the achievable highest R_C is ~40 Gchip/s, which corresponds to a minimum D of ~712 and ~178 ps/nm for 10 and 40 Gb/s, respectively. In the experiment, the total dispersion of the LCFBGs is ~240 ps/nm, which is higher than the minimum D for 40 Gb/s but lower than that of the 10 Gb/s, so security enhancement for 40 Gb/s can be expected.

Three different codes with code lengths of 128, 512, and 1024 are used in the en/decoding experiment. These codes are randomly selected from Gold codes with different chips plus a zero. Figures 4(a) and 4(b) show the correctly decoded waveform and corresponding eye diagram for the 40 Gb/s OOK pulse train with a 1024-chip OC. Autocorrelation short pulses with high peak power and clear eye opening have been obtained after correctly decoding. However, as shown in Figs. 4(c) and 4(d), using the correct opposite dispersive LCFBGs but incorrect OC, the decoded waveform exhibits as a noiselike signal, and no eye opening can be observed in the corresponding eye diagram. It is unable to distinguish the symbol "1" and "0" from the waveform, showing that the eavesdropper cannot easily intercept the data by simple power detection if he has no knowledge of the applied fast reconfigurable, ultralong OC. Figures 4(e) and 4(f) show the incorrectly decoded waveform and corresponding eye diagram for R_C of 10 Gchip/s. In this case, the symbols "1" and "0" are distinguishable and the eye diagram has opening. This is due to the fact that the time duration T_{cr} for each bit after LCFBGs compressing corresponds to ~34 ps for the 40 Gchip/s chip modulation rate, and thus the adjacent incorrectly decoded pulses have significant symbol overlapping for the 40 Gb/s data rate, while for the R_C of 10 Gchip/s corresponding to a T_{cr} of ~8.5 ps, there is no significant symbol overlapping. Similarly, for the 10 Gb/s data rate and 40 Gchip/s chip modulation rate, as the T_{cr} is smaller than the bit period, it is still possible for the eavesdropper to intercept the data by using power detection even without the OC, as can be seen from the waveform and clear eye diagram shown in Figs. 4(g) and 4(h). By further increasing the dispersion D and R_C, security improvement for the 10 Gb/s data rate could also be expected.

The behavior of a 40 Gb/s data pattern stream 10101010111111010110 has also been observed, as shown in Figs. 5(a)–5(c). It can be seen that, for the low R_C of 10 Gchip/s in Fig. 5(b), the data pattern can still be extracted from the encoded waveform, while for the higher R_C of 40 Gchip/s in Fig. 5(c), the data pulses have been spread in time domain and distorted, which makes it hard to extract the pattern using a simple power detector. The BER performances for the correctly decoded and demultiplexed four-channel 10 Gb/s OOK tributaries are shown in Fig. 5(d). Error-free transmission has been achieved for all the tributaries with the three codes. Compared with the case without en/decoding, the average power penalty at BER $= 10^{-9}$ for the three codes is around 1 dB due to the nonideal decoding for every bit. As for the cross-correlation signals, no BER can be measured, indicating significant enhancement of the 40 Gb/s OOK data security based on the time domain SPE/D scheme with symbol overlapping.

In conclusion, we have proposed and demonstrated, first to our knowledge, a 40 Gb/s fast reconfigurable time domain SPE/D OOK optical communication system secured by the symbol overlapping of encoded and incorrectly decoded signals and 40 Gchip/s code-length variable ultralong OCs of up to 1024 chips. The proposed scheme is very robust to malicious eavesdropping using power detection, and thus it can significantly improve the information security. It has the potential to support longer code length, higher transmission speed, and is compatible with other approaches for secure optical communication.

References

1. S. Etemad, A. Agarwal, T. Banwell, G. Crescenzo, J. Jackel, R. Menendez, and P. Toliver, IEEE Commun. Mag. **46**(8), 32 (2008).
2. N. Gisin and R. Thew, Nat. Photon. **1**, 165 (2007).
3. V. Annovzzi-Lodi, A. Argyris, M. Benedetti, M. Hamacher, S. Merlo, and D. Syvridis, Opt. Photon. News **19**(10), 36 (2008).
4. M. P. Fok and P. R. Prucnal, Electron. Lett. **45**, 179 (2009).
5. T. H. Shake, J. Lightwave Technol. **23**, 655 (2005).
6. Y. Du, F. Xue, S. J. B. Yoo, and Z. Ding, J. Lightwave Technol. **25**, 2799 (2007).
7. Z. Gao, B. Dai, X. Wang, N. Kataoka, and N. Wada, Opt. Lett. **36**, 1623 (2011).
8. Z. Jiang, D. S. Seo, S.-D. Yang, D. E. Leaird, R. V. Roussev, C. Langrock M. M. Fejer, and A. M. Weiner, J. Lightwave Technol. **23**, 143 (2005).
9. Z. Si, F. Yin, M. Xin, H. Chen, M. Chen, and S. Xie, Opt. Lett. **35**, 229 (2010).
10. J. P. Heritage and A. M. Weiner, IEEE J. Quantum Electron. **13**, 1351 (2007).
11. P. Lazaridis, G. Debarge, and P. Gallion, Opt. Lett. **20**, 1160 (1995).